- benötigte Authentisierungsfunktionen des Terminalserver-Protokolls
- Möglichkeit zum Anzeigen der Ausgabe fremder Sitzungen
- Kommunikation zwischen Anwendungen in den Terminalserver-Sitzungen und Anwendungen auf anderen Servern
- Kommunikation zwischen Terminalserver und anderen Servern

SYS.1.9.A5 Planung der eingesetzten Clients und Terminal-Client-Software (B)

Es MUSS festgelegt werden, über welche Terminal-Client-Software auf den Terminalserver zugegriffen werden darf. Zusätzlich MUSS festgelegt werden, auf welchen Clients diese Software ausgeführt werden darf, um sich mit dem Terminalserver zu verbinden. Hierbei MÜSSEN mindestens die folgenden Punkte berücksichtigt werden:

- Einsatz von Thin Clients oder Fat Clients,
- Hardware-Konfiguration der zugreifenden Clients sowie
- Betriebssystem der zugreifenden Clients.

Es MUSS festgelegt werden, welche Software neben der Terminal-Client-Software zusätzlich auf den Clients zugelassen ist. Zusätzlich MUSS festgelegt werden, ob ein Client parallel Anwendungen auf unterschiedlichen Terminalservern benutzen darf.

SYS.1.9.A6 Planung der verwendeten Netze (B) [Planende]

Die Netze, über die Clients mit Terminalservern kommunizieren, MÜSSEN anhand der Anforderungen der bereitgestellten Anwendungen geplant und gegebenenfalls angepasst werden. Hierbei MÜSSEN mindestens folgende Punkte berücksichtigt werden:

- zu erwartende Anzahl gleichzeitiger Terminalserver-Sitzungen,
- benötigte Übertragungskapazität,
- maximal vertretbarer Paketverlust,
- maximal vertretbarer Jitter sowie
- maximal tolerierbare Latenzzeit des Netzes.

SYS.1.9.A7 Sicherer Zugriff auf den Terminalserver (B)

Es MUSS festgelegt werden, über welche Netze zwischen zugreifendem Client und Terminalserver kommuniziert werden darf. Zusätzlich MUSS festgelegt werden, wie die Kommunikation abgesichert werden soll. Es MUSS festgelegt werden, ob und wie mit dem Terminalserver-Protokoll verschlüsselt werden soll. Falls das Terminalserver-Protokoll in diesem Fall keine ausreichende Verschlüsselung bietet, MUSS die Kommunikation zusätzlich abgesichert werden.

Falls die Clients und der Terminalserver über unzureichend vertrauenswürdige Netze kommunizieren, MÜSSEN sich sowohl die Benutzenden als auch der Terminalserver beim Kommunikationsaufbau authentisieren.

SYS.1.9.A8 Sichere Zuordnung des Terminalservers zu Netzsegmenten (B)

Der Terminalserver MUSS in dedizierten Netzsegmenten oder in Client-Netzsegmenten positioniert werden. Innerhalb von Client-Netzsegmenten MÜSSEN Terminalserver identifizierbar sein.

Eine bestehende Netztrennung DARF NICHT über einen Terminalserver umgangen werden können.

SYS.1.9.A9 Sensibilisierung der Benutzenden (B)

Alle Benutzenden von Terminalservern MÜSSEN über den sicheren Umgang mit Terminalservern sensibilisiert werden. Den Benutzenden MÜSSEN mindestens die folgenden Inhalte vermittelt werden:

- grundsätzliche Funktionsweise und die Auswirkungen von Latenz und verfügbarer Bandbreite auf die Bedienbarkeit
- mögliche und erlaubte Speicherorte von Daten

- zugelassene Austauschmöglichkeiten von Informationen zwischen dem Betriebssystem des Clients und dem Terminalserver (z. B. Zwischenablage)
- Auswirkung des eigenen Ressourcenverbrauchs auf die zur Verfügung stehenden Ressourcen für andere Benutzende
- eingerichtete Rollen und Berechtigungen für Terminalserver-Zugriffe
- genutzte Authentisierung und Autorisierung der Benutzenden für die zur Verfügung gestellten Anwendungen
- maximale Sitzungsdauer und automatische Abmeldevorgänge

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.9.A10 Einsatz eines zentralen Identitäts- und Berechtigungsmanagements für Terminalserver (S)

Für die Benutzung von Terminalservern SOLLTE ein zentrales System zum Identitäts- und Berechtigungsmanagement eingesetzt werden.

SYS.1.9.A11 Sichere Konfiguration von Profilen (S)

Benutzende SOLLTEN ihre spezifischen Einstellungen (Benutzendenprofile) NICHT derart ändern dürfen, dass die Informationssicherheit oder die Nutzung des Terminalservers eingeschränkt wird. Für die Benutzendenprofile SOLLTE eine geeignete maximale Größe festgelegt werden. Wenn Verbünde aus Terminalservern eingesetzt werden, SOLLTEN die Benutzendenprofile zentral abgelegt werden.

SYS.1.9.A12 Automatisches Beenden inaktiver Sitzungen (S)

Inaktive Sitzungen auf Terminalservern SOLLTEN nach einem vordefinierten Zeitraum beendet werden. Der Zeitraum, während dessen eine Sitzung maximal aktiv bleiben soll, SOLLTE abhängig von der jeweiligen Benutzendengruppe festgelegt werden. Falls eine Sitzung automatisch beendet wird, SOLLTEN die Betroffenen darüber benachrichtigt werden. Wenn eine Sitzung beendet wird, SOLLTE auch der oder die Benutzende automatisch vom Betriebssystem des Terminalservers abgemeldet werden, sofern die Sitzung am Betriebssystem nicht weiterhin für laufende Anwendungen benötigt wird.

SYS.1.9.A13 Protokollierung bei Terminalservern (S)

Für die Terminalserver SOLLTE entschieden werden, welche Ereignisse an eine zentrale Protokollierungsinfrastruktur (siehe OPS.1.1.5 *Protokollierung)* übermittelt werden sollen. Hierbei SOLLTEN mindestens die folgenden spezifischen Ereignisse an Terminalservern protokolliert werden:

- Anbindung von Peripheriegeräten der zugreifenden Clients über das Terminalserver-Protokoll,
- Aktionen auf dem Terminalserver durch zugreifende Clients, die erweiterte Rechte benötigen sowie
- Konfigurationsänderungen mit Auswirkungen auf den Terminalserver-Dienst.

SYS.1.9.A14 Monitoring des Terminalservers (S)

Der Terminalserver SOLLTE zentral überwacht werden. Hierfür SOLLTEN mindestens folgende Parameter überwacht werden:

- Auslastung der Ressourcen des Terminalservers,
- Auslastung der Netzschnittstellen des Terminalservers,
- verfügbare und genutzte Bandbreite der verbundenen Clients sowie
- Latenz an den verbundenen Clients unter Berücksichtigung der jeweiligen Anforderungsprofile.

Für das Monitoring SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining). Diese Schwellwerte SOLLTEN regelmäßig überprüft und bei Bedarf angepasst werden.

SYS.1.9.A15 Härtung des Terminalservers (S)

Nicht benötigte Anwendungen auf dem Terminalserver SOLLTEN entfernt werden. Ist das nicht möglich, SOLLTE deren Ausführung unterbunden werden.

Der Zugriff aus einer Sitzung auf Peripheriegeräte SOLLTE auf die benötigten Geräte eingeschränkt werden.

SYS.1.9.A16 Optimierung der Kompression (S)

Der Grad der Kompression bei der Übertragung der Daten von und zum Terminalserver SOLLTE entsprechend der Anforderungen der jeweiligen Anwendung an die grafische Qualität optimiert werden. Die Anforderungen der bereitgestellten Anwendungen an Genauigkeit von grafischen Elementen, an Farbtreue und die für die Nutzung notwendige Bildrate SOLLTEN berücksichtigt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.1.9.A17 Verschlüsselung der Übertragung (H)

Jegliche Kommunikation zwischen Client und Terminalserver SOLLTE geeignet verschlüsselt werden. Dabei SOLLTEN sichere Protokolle gemäß BSI TR-02102 verwendet werden.

SYS.1.9.A18 Nutzung von Thin Clients (H)

Physische Thin Clients SOLLTEN verwendet werden. Es SOLLTEN nur Thin Clients eingesetzt werden, die das Unternehmen, das die Terminal-Client-Software herstellt, als kompatibel ausgewiesen hat.

SYS.1.9.A19 Erweitertes Monitoring des Terminalservers (H)

Für den Terminalserver SOLLTE kontinuierlich überwacht werden, ob die in SYS.1.9.A13 *Protokollierung bei Terminalservern* beschriebenen Ereignisse auftreten.

Wird ein Security Information and Event Management (SIEM) genutzt, SOLLTE der Terminalserver darin eingebunden werden. Im SIEM SOLLTEN die überwachten Ereignisse hinsichtlich Anomalien inklusive Angriffsmustern automatisiert analysiert werden.

Der Terminalserver SOLLTE regelmäßig auf Schwachstellen überprüft werden.

SYS.1.9.A20 Unterschiedliche Terminalserver für unterschiedliche Gruppen von Benutzenden oder Geschäftsprozesse (H)

Die Benutzenden von Terminalservern SOLLTEN anhand ähnlicher Berechtigungen und benötigter Anwendungen gruppiert werden. Ein Terminalserver SOLLTE NICHT mehreren Gruppen von Benutzenden zur Verfügung gestellt werden. Ist dies nicht möglich, SOLLTEN dedizierte Terminalserver pro Geschäftsprozess eingesetzt werden.

SYS.1.9.A21 Nutzung hochverfügbarer IT-Systeme (H)

Der Terminalserver SOLLTE hochverfügbar betrieben werden. Dazu SOLLTEN der Terminalserver sowie dessen Netzanbindung redundant ausgelegt werden. Die verwendeten Terminalserver SOLLTEN im Verbund betrieben werden. Für die zugreifenden Clients SOLLTEN Ersatzgeräte bereitgehalten werden.

SYS.1.9.A22 Unterbinden des Transfers von Anwendungsdaten zwischen Client und Terminalserver (H)

Der Transfer von Anwendungsdaten zwischen dem Client und dem Terminalserver SOLLTE deaktiviert werden. Auch der Transfer der Zwischenablage SOLLTE deaktiviert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102“ Hinweise zur Anwendung kryptografischer Verfahren zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Empfehlungen für den sicheren Einsatz von Application Delivery Controllern (ADC)“ Hinweise für den sicheren Einsatz von ADC zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.1 Allgemeiner Client

1. Beschreibung

1.1. Einleitung

Als „Allgemeiner Client" wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzenden zulässt und nicht dazu dient, Server-Dienste bereitzustellen. Auf einem Client sollten mindestens getrennte Umgebungen zur Administration und zur Benutzung eingerichtet werden können. Das IT-System verfügt in der Regel über Laufwerke und Anschlussmöglichkeiten für externe bzw. wechselbare Datenträger, weitere Schnittstellen für den Datenaustausch sowie andere Peripheriegeräte. Typischerweise ist ein solches IT-System in ein Client-Server-Netz eingebunden. Bei dem IT-System kann es sich beispielsweise um einen PC mit oder ohne Festplatte, um ein mobiles oder stationäres Gerät, aber auch um eine Linux-Workstation oder einen Apple Mac handeln.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf jeglicher Art von Clients, unabhängig vom verwendeten Betriebssystem, erstellt, gelesen, bearbeitet, gespeichert oder versendet werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.1 *Allgemeiner Client* ist für alle Clients unabhängig vom konkreten Betriebssystem anzuwenden.

In der Regel werden Clients unter einem Betriebssystem ausgeführt, das jeweils eigene Sicherheitsmaßnahmen erfordert. Für verbreitete Client-Betriebssysteme sind spezifische Bausteine in der Schicht SYS.2 *Desktop-Systeme* vorhanden, die auf dem vorliegenden Baustein aufbauen und zusätzlich anzuwenden sind. Falls für eingesetzte Clients kein spezifischer Baustein existiert, müssen die Anforderungen des vorliegenden Bausteins geeignet für das Zielobjekt konkretisiert und es muss eine ergänzende Risikobetrachtung durchgeführt werden.

Sicherheitsempfehlungen für mobile Endgeräte mit festem Betriebssystem, wie Smartphones oder Tablets, sind in der Schicht SYS.3 *Mobile Devices* zu finden. Falls ein Client weitere Schnittstellen zum Datenaustausch hat, wie z. B. USB, Bluetooth, LAN oder WLAN, müssen diese gemäß den Sicherheitsvorgaben der Institution so abgesichert werden, wie es in den entsprechenden Bausteinen beschrieben ist. Hierzu sind Anforderungen beispielsweise in SYS.4.5 *Wechseldatenträger* oder NET.2.2 *WLAN-Nutzung* zu finden.

Regelmäßig sind außerdem die Anforderungen der Bausteine OPS.1.1.3 *Patch- und Änderungsmanagement* und CON.3 *Datensicherungskonzept* für Clients zu berücksichtigen. Clients sind oft durch Schadsoftware gefährdet, daher sind die Anforderungen des Bausteins OPS.1.1.4 *Schutz vor Schadprogrammen* bei Clients besonders relevant.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.2.1 *Allgemeiner Client* von besonderer Bedeutung.

2.1. Schadprogramme

Schadprogramme werden mit dem Ziel entwickelt, unerwünschte und schädliche Funktionen auf IT-Systemen auszuführen. Sie werden meist „heimlich" aktiv, d. h. ohne, dass die Benutzenden davon wissen oder darin einwilligen. Je nach Ausprägung bieten sie bei Angriffen umfangreiche Kommunikations- und Steuerungsmöglichkeiten mit vielen unterschiedlichen Funktionen. Unter anderem könnten sie gezielt Passwörter auslesen, IT-Systeme fernsteuern, Schutzsoftware deaktivieren, Daten ausspionieren oder verschlüsseln.

Clients sind besonders anfällig für Schadsoftware. Sie werden direkt von den Benutzenden bedient und sind somit oft das Einfallstor für schädliche Inhalte jeglicher Art. Besuchen die Benutzenden bösartige Webseiten, öffnen E-Mails mit schädlichem Inhalt von privaten Konten oder kopieren Schadsoftware über lokale Datenträger auf den Client, kann sich so die Schadsoftware über die Clients in das Netz der Institution verbreiten. Zentrale Schutzmechanismen, wie z. B. ein Virenschutz auf dem Datei- oder E-Mail-Server, können so oft umgangen werden.

2.2. Datenverlust durch lokale Datenhaltung

Trotz regelmäßiger, gegensätzlicher Empfehlung werden oft auch wichtige Daten ausschließlich lokal abgespeichert. Beispielsweise werden Daten häufig in lokalen Verzeichnissen abgelegt, statt auf einem zentralen Dateiserver. Auch E-Mails werden häufig nur lokal archiviert. So können etwa bei Hardwaredefekten leicht Daten verloren gehen. Werden für die Institution wichtige Daten zerstört oder verfälscht, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder sogar ganz verhindert werden. Insgesamt kann der Verlust gespeicherter Daten neben einem Arbeitsausfall und den Kosten für eine Wiederbeschaffung auch zu langfristigen Konsequenzen wie beispielsweise Vertrauenseinbußen bei Geschäftsbeziehungen sowie einem negativen Eindruck in der Öffentlichkeit führen. Durch die von den durch Datenverluste verursachten direkten und indirekten Schäden können Institutionen im Extremfall in ihrer Existenz bedroht sein.

Werden wichtige Daten ausschließlich lokal gehalten, können andere Personen außerdem nicht darauf zugreifen, etwa im Vertretungsfall bei Urlaub oder Krankheit.

Auch wenn grundsätzliche Vorgaben zur zentralen Speicherung eingehalten werden, werden oftmals zusätzlich lokale Kopien der zentral gespeicherten Daten angelegt. Dies führt nicht nur häufig zu inkonsistenten Versionsständen, sondern auch dazu, dass Daten entweder vorschnell oder nicht wie notwendig gelöscht werden.

2.3. Hardware-Defekte bei Client-Systemen

Anders als bei zentralen IT-Systemen wie Servern, arbeiten Benutzende bei Clients direkt am oder mit dem Endgerät. Dadurch könnten sie den Client unter Umständen gewollt oder ungewollt beschädigen. Beispielsweise könnten sie gegen auf dem Boden stehende IT-Systeme treten, über Kabel stolpern und damit Schnittstellen beschädigen oder Flüssigkeiten über Geräte verschütten. Gibt es keinen schnellen Ersatz, kann das IT-System bis zum Abschluss der Reparatur nicht bestimmungsgemäß eingesetzt werden. Fällt ein mobiles Gerät wie ein Laptop unterwegs aus, kann die Arbeit oft erst nach der Rückkehr in die Institution fortgesetzt werden.

2.4. Unberechtigte Nutzung von Clients

Die Identifikation und Authentisierung von Personen soll verhindern, dass ein Client unberechtigt verwendet wird. Aber auch IT-Systeme, bei denen sich Benutzende über IDs und Passwörter identifizieren und authentisieren müssen, können unberechtigt genutzt werden, wenn es Angreifenden gelingt, die Zugangsdaten auszuspähen oder zu erraten. Wird keine Bildschirmsperre aktiviert, kann der Client auch bei kurzzeitiger Abwesenheit unberechtigt genutzt werden.

2.5. Installation nicht benötigter Betriebssystemkomponenten und Applikationen

Bei der Installation eines Betriebssystems besteht in der Regel die Möglichkeit, optionale Software zu installieren. Auch im laufenden Betrieb wird regelmäßig Software installiert und getestet. Mit jeder weiteren Anwendung steigen nicht nur Rechen- und Speicherlast eines Clients an, sondern auch die Wahrscheinlichkeit für darin verborgene Schwachstellen. Nicht benötigte Software unterliegt außerdem häufig keinem regelmäßigen Patch-Management, sodass auch bekannte Sicherheitslücken nicht zeitnah geschlossen werden. Dadurch können solche Schwachstellen für Angriffe ausgenutzt werden.

2.6. Abhören von Räumen mittels Mikrofon und Kamera

Viele Clients verfügen über ein Mikrofon und eine Kamera. Diese können prinzipiell von jedem aktiviert und verwendet werden, der über entsprechende Zugriffsrechte verfügt, bei vernetzten Systemen auch von Externen. Werden diese Rechte nicht sorgfältig vergeben, können Unbefugte Mikrofon oder Kamera dazu missbrauchen, um über das Internet Räume abzuhören oder unbemerkt Besprechungen aufzuzeichnen. Hierzu gehören auch Intelligente Persönliche Assistenten (IPA) oder Sprachassistenten, die die Umgebung permanent abhören und nach Nennung eines geräteabhängigen Aktivierungsworts bestimmte Funktionen ausführen, wie Musik abspielen, Kontakte anrufen, die Beleuchtung steuern oder das Raumklima verändern. Werden die Gespräche z. B. von IPAs an Dritte übermittelt, könnten diese unter Umständen von Unbefugten abgehört werden. Die aufgezeichneten Gespräche könnten auch bei den herstellenden Unternehmen von IPAs längerfristig abgespeichert und weiterverarbeitet werden.

2.7. Fehlerhafte Administration oder Nutzung von Geräten und Systemen

Moderne Client-Betriebssysteme sind sehr komplex. Daher können insbesondere Fehlkonfiguration von Komponenten die Sicherheit beeinträchtigen, sodass das IT-System fehlerhaft funktioniert oder kompromittiert werden kann. Grundsätzlich beinhaltet jede Schnittstelle an einem IT-System nicht nur die Möglichkeit, darüber bestimmte Dienste des IT-Systems berechtigt zu nutzen, sondern auch das Risiko, dass Unbefugte auf das IT-System zugreifen. Wenn etwa durch Fehlkonfiguration der Authentisierungsmechanismen Kennungen und zugehörige Passwörter ausgespäht werden können, ist eine unberechtigte Nutzung der damit geschützten Anwendungen oder IT-Systeme denkbar.

Auch eine fehlerhafte oder nicht ordnungsgemäße Nutzung von Geräten, Systemen und Anwendungen kann die Sicherheit beeinträchtigen, vor allem, wenn vorhandene Sicherheitsmaßnahmen missachtet oder umgangen werden. So können beispielsweise zu großzügig vergebene Rechte, leicht zu erratende Passwörter, nicht ausreichend geschützte Datenträger mit Sicherungskopien oder bei vorübergehender Abwesenheit nicht gesperrte Arbeitsplätze zu Sicherheitsvorfällen führen. Eine weitere Folge der fehlerhaften Bedienung von IT-Systemen oder Anwendungen kann das versehentlich Löschen oder Verändern von Daten sein. Dabei ist es ebenfalls möglich, dass vertrauliche Informationen in die Hände Dritter gelangen, beispielsweise wenn Zugriffsrechte falsch gesetzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.1 *Allgemeiner Client* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.2.1.A1 Sichere Authentisierung von Benutzenden (B)

Um den Client zu nutzen, MÜSSEN sich die Benutzenden gegenüber dem IT-System authentisieren. Benutzende MÜSSEN eine Bildschirmsperre verwenden, wenn sie den Client unbeaufsichtigt betreiben. Die Bildschirmsperre SOLLTE automatisch aktiviert werden, wenn für eine festgelegte Zeitspanne keine Aktion durch Benutzende durch-

geführt wurde. Die Bildschirmsperre DARF NUR durch eine erfolgreiche Authentisierung wieder deaktiviert werden können. Benutzende SOLLTEN verpflichtet werden, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

SYS.2.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen (B)

Automatische Update-Mechanismen (Autoupdate) MÜSSEN aktiviert werden, sofern nicht andere Mechanismen wie regelmäßige manuelle Wartung oder ein zentrales Softwareverteilungssystem für Updates eingesetzt werden. Wenn für Autoupdate-Mechanismen ein Zeitintervall vorgegeben werden kann, SOLLTE mindestens täglich automatisch nach Updates gesucht und diese installiert werden.

SYS.2.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.2.1.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.2.1.A6 Einsatz von Schutzprogrammen gegen Schadsoftware (B)

Abhängig vom installierten Betriebssystem und von anderen vorhandenen Schutzmechanismen des Clients MUSS geprüft werden, ob Schutzprogramme gegen Schadsoftware eingesetzt werden sollen. Soweit vorhanden, MÜSSEN konkrete Aussagen, ob ein solcher Schutz notwendig ist, aus den spezifischen Betriebssystem-Bausteinen des IT-Grundschutz-Kompendiums berücksichtigt werden.

Schutzprogramme auf den Clients MÜSSEN so konfiguriert sein, dass Benutzende weder sicherheitsrelevante Änderungen an den Einstellungen vornehmen noch die Schutzprogramme deaktivieren können.

Das Schutzprogramm MUSS nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen werden. Der gesamte Datenbestand eines Clients MUSS regelmäßig auf Schadsoftware geprüft werden. Wenn ein Client infiziert ist, MUSS im Offlinebetrieb untersucht werden, ob ein gefundenes Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

SYS.2.1.A7 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.2.1.A8 Absicherung des Bootvorgangs (B)

Der Startvorgang des IT-Systems („Booten“) MUSS gegen Manipulation abgesichert werden. Es MUSS festgelegt werden, von welchen Medien gebootet werden darf. Es SOLLTE entschieden werden, ob und wie der Bootvorgang kryptografisch geschützt werden soll. Es MUSS sichergestellt werden, dass nur Administrierende die Clients von einem anderen als den voreingestellten Laufwerken oder externen Speichermedien booten können. NUR Administrierende DÜRFEN von wechselbaren oder externen Speichermedien booten können. Die Konfigurationseinstellungen des Bootvorgangs DÜRFEN NUR durch Administrierende verändert werden können. Alle nicht benötigten Funktionen in der Firmware des Client-Systems MÜSSEN deaktiviert werden.

SYS.2.1.A42 Nutzung von Cloud- und Online-Funktionen (B) [Benutzende]

Es DÜRFEN NUR zwingend notwendige Cloud- und Online-Funktionen des Betriebssystems genutzt werden. Die notwendigen Cloud- und Online-Funktionen SOLLTEN dokumentiert werden. Die entsprechenden Einstellungen des Betriebssystems MÜSSEN auf Konformität mit den organisatorischen Datenschutz- und Sicherheitsvorgaben überprüft und restriktiv konfiguriert bzw. die Funktionen deaktiviert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.1.A9 Festlegung einer Sicherheitsrichtlinie für Clients (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an allgemeine Clients konkretisiert werden. Die Richtlinie SOLLTE allen Benutzenden sowie allen Personen, die an der Beschaffung und dem Betrieb der Clients beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert werden.

SYS.2.1.A10 Planung des Einsatzes von Clients (S)

Es SOLLTE im Vorfeld geplant werden, wo und wie Clients eingesetzt werden sollen. Die Planung SOLLTE dabei nicht nur Aspekte betreffen, die typischerweise direkt mit den Begriffen IT- oder Informationssicherheit in Verbindung gebracht werden, sondern auch betriebliche Aspekte, die Anforderungen im Bereich der Sicherheit nach sich ziehen. Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.2.1.A11 Beschaffung von Clients (S)

Bevor Clients beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Die jeweiligen herstellenden Unternehmen von IT- und Betriebssystem SOLLTEN für den gesamten geplanten Nutzungszeitraum Patches für Schwachstellen zeitnah zur Verfügung stellen. Auf Betriebssysteme, die über ein Rolling-Release-Modell aktualisiert werden, SOLLTE verzichtet werden. Die zu beschaffenden Systeme SOLLTEN über eine Firmware-Konfigurationsoberfläche für UEFI SecureBoot und, sofern vorhanden, für das TPM verfügen, die eine Kontrolle durch die Institution gewährleistet und so den selbstverwalteten Betrieb von SecureBoot und des TPM ermöglicht.

SYS.2.1.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A13 Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (S)

Der Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung (z. B. durch das Betriebssystem speziell abgesicherte Speicherbereiche, Firmwarebereiche etc.) SOLLTE nur mit administrativen Berechtigungen möglich sein. Die entsprechenden Einstellungen im BIOS bzw. der UEFI-Firmware SOLLTEN durch ein Passwort vor unberechtigten Veränderungen geschützt werden. Wird die Kontrolle über die Funktionen an das Betriebssystem delegiert, SOLLTEN auch dort nur mit administrativen Berechtigungen auf die Funktionen zugegriffen werden dürfen.

SYS.2.1.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A15 Sichere Installation und Konfiguration von Clients (S)

Es SOLLTE festgelegt werden, welche Komponenten des Betriebssystems, welche Fachanwendungen und welche weiteren Tools installiert werden sollen. Die Installation und Konfiguration der IT-Systeme SOLLTE nur von autorisierten Personen (Administrierende oder vertraglich gebundene Dienstleistende) nach einem definierten Prozess in einer Installationsumgebung durchgeführt werden. Nachdem die Installation und die Konfiguration abgeschlossen sind, SOLLTEN die Grundeinstellungen überprüft werden. Sofern die Installation und Konfiguration den Vorgaben aus der Sicherheitsrichtlinie entsprechen, SOLLTEN die Clients im Anschluss in der Produktivumgebung in Betrieb genommen werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass diese durch sachkundige Dritte nachvollzogen und wiederholt werden können.

SYS.2.1.A16 Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen (S)

Nach der Installation SOLLTE überprüft werden, welche Komponenten der Firmware sowie des Betriebssystems und welche Anwendungen und weiteren Tools auf den Clients installiert und aktiviert sind. Nicht benötigte Module, Programme, Dienste, Aufgaben und Firmwarefunktionen (wie Fernwartung) SOLLTEN deaktiviert oder ganz deinstalliert werden. Nicht benötigte Laufzeitumgebungen, Interpretersprachen und Compiler SOLLTEN deinstalliert werden. Nicht benötigte Kennungen SOLLTEN deaktiviert oder gelöscht werden. Nicht benötigte Schnittstellen und Hardware des IT-Systems (wie z. B. Webcams) SOLLTEN deaktiviert werden. Es SOLLTE verhindert werden, dass diese

Komponenten wieder reaktiviert werden können. Die getroffenen Entscheidungen SOLLTEN nachvollziehbar dokumentiert werden.

SYS.2.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A18 Nutzung von verschlüsselten Kommunikationsverbindungen (S)

Kommunikationsverbindungen SOLLTEN, soweit möglich, durch Verschlüsselung geschützt werden.

Die Clients SOLLTEN kryptografische Algorithmen und Schlüssellängen verwenden, die dem Stand der Technik und den Sicherheitsanforderungen der Institution entsprechen.

Neue Zertifikate von Zertifikatsausstellern SOLLTEN erst nach Überprüfung des Fingerprints aktiviert werden.

SYS.2.1.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A20 Schutz der Administrationsverfahren bei Clients (S)

Abhängig davon, ob Clients lokal oder über das Netz administriert werden, SOLLTEN geeignete Sicherheitsvorkehrungen getroffen werden. Die zur Administration verwendeten Verfahren SOLLTEN über die in der Sicherheitsrichtlinie festgelegten Vorgaben erfolgen.

SYS.2.1.A21 Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras (S)

Der Zugriff auf Mikrofon und Kamera eines Clients SOLLTE nur durch Benutzende selbst möglich sein, solange sie lokal am IT-System arbeiten. Wenn vorhandene Mikrofone oder Kameras nicht genutzt und deren Missbrauch verhindert werden soll, SOLLTEN diese, wenn möglich, ausgeschaltet, abgedeckt (nur Kamera), deaktiviert oder physisch vom Gerät getrennt werden. Es SOLLTE geregelt werden, wie Kameras und Mikrofone in Clients genutzt und wie die Rechte vergeben werden.

SYS.2.1.A22 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A23 Bevorzugung von Client-Server-Diensten (S)

Wenn möglich, SOLLTEN zum Informationsaustausch dedizierte Serverdienste genutzt und direkte Verbindungen zwischen Clients vermieden werden. Falls dies nicht möglich ist, SOLLTE festgelegt werden, welche Client-zu-Client-Dienste (oft auch als „Peer-to-Peer" bezeichnet) genutzt und welche Informationen darüber ausgetauscht werden dürfen. Falls erforderlich, SOLLTEN Benutzende für die Nutzung solcher Dienste geschult werden. Direkte Verbindungen zwischen Clients SOLLTEN sich nur auf das LAN beschränken. Auto-Discovery-Protokolle SOLLTEN auf das notwendige Maß beschränkt werden.

SYS.2.1.A24 Umgang mit externen Medien und Wechseldatenträgern (S)

Auf externe Schnittstellen SOLLTE nur restriktiv zugegriffen werden können. Es SOLLTE untersagt werden, dass nicht zugelassene Geräte oder Wechseldatenträger mit den Clients verbunden werden. Es SOLLTE verhindert werden, dass von den Clients auf Wechseldatenträger aus nicht vertrauenswürdigen Quellen zugegriffen werden kann. Die unerlaubte Ausführung von Programmen auf bzw. von externen Datenträgern SOLLTE technisch unterbunden werden. Es SOLLTE verhindert werden, dass über Wechsellaufwerke oder externe Schnittstellen unberechtigt Daten von den Clients kopiert werden können.

SYS.2.1.A25 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.1.A26 Schutz vor Ausnutzung von Schwachstellen in Anwendungen (S)

Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, SOLLTEN ASLR und DEP/NX im Betriebssystem aktiviert und von den Anwendungen genutzt werden. Sicherheitsfunktionen des Kernels und der Standardbibliotheken wie z. B. Heap- und Stackschutz SOLLTEN aktiviert werden.

SYS.2.1.A27 Geregelte Außerbetriebnahme eines Clients (S)

Bei der Außerbetriebnahme eines Clients SOLLTE sichergestellt werden, dass keine Daten verloren gehen und dass keine schutzbedürftigen Daten zurückbleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf den IT-Systemen gespeichert sind. Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines IT-Systems abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung weiterhin benötigter Daten und dem anschließenden sicheren Löschen aller Daten umfassen.

SYS.2.1.A34 Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten (S)

Um sowohl den Zugriff auf das Betriebssystem oder andere Anwendungen bei Angriffen als auch den Zugriff vom Betriebssystem auf besonders schützenswerte Dateien zu verhindern, SOLLTEN Anwendungen und Betriebssystemkomponenten (wie beispielsweise Authentisierung oder Zertifikatsüberprüfung) ihrem Schutzbedarf entsprechend besonders gekapselt bzw. anderen Anwendungen und Betriebssystemkomponenten gegenüber isoliert werden. Dabei SOLLTEN insbesondere sicherheitskritische Anwendungen berücksichtigt werden, die mit Daten aus unsicheren Quellen arbeiten (z. B. Webbrowser und Bürokommunikations-Anwendungen).

SYS.2.1.A43 Lokale Sicherheitsrichtlinien für Clients (S)

Alle sicherheitsrelevanten Einstellungen SOLLTEN bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Dafür SOLLTEN Sicherheitsrichtlinien, unter Berücksichtigung der Empfehlungen des herstellenden Unternehmens und des voreingestellten Standardverhaltens, konfiguriert werden, sofern das Standardverhalten nicht anderen Anforderungen aus dem IT-Grundschutz oder der Organisation widerspricht. Die Entscheidungen SOLLTEN dokumentiert und begründet werden. Sicherheitsrichtlinien SOLLTEN in jedem Fall gesetzt werden, auch dann, wenn das voreingestellte Standardverhalten dadurch nicht verändert wird.

SYS.2.1.A44 Verwaltung der Sicherheitsrichtlinien von Clients (S)

Alle Einstellungen der Clients SOLLTEN durch Nutzung eines Managementsystems verwaltet und entsprechend dem ermittelten Schutzbedarf sowie auf den internen Richtlinien basierend konfiguriert sein. Konfigurationsänderungen SOLLTEN dokumentiert, begründet und mit dem Sicherheitsmanagement abgestimmt werden, sodass der Stand der Sicherheitskonfiguration jederzeit nachvollziehbar ist und Konfigurationsänderungen schnell durchgeführt und zentralisiert verteilt werden können.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.2.1.A28 Verschlüsselung der Clients (H)

Wenn vertrauliche Informationen auf den Clients gespeichert werden, SOLLTEN mindestens die schutzbedürftigen Dateien sowie ausgewählte Dateisystembereiche oder besser die gesamten Datenträger verschlüsselt werden. Hierfür SOLLTE ein eigenes Konzept erstellt und die Details der Konfiguration besonders sorgfältig dokumentiert werden. In diesem Zusammenhang SOLLTEN die Authentisierung (z. B. Passwort, PIN, Token), die Ablage der Wiederherstellungsinformationen, die zu verschlüsselnden Laufwerke und die Schreibrechte auf unverschlüsselte Datenträger geregelt werden. Der Zugriff auf das genutzte Schlüsselmaterial MUSS angemessen geschützt sein.

Benutzende SOLLTEN darüber aufgeklärt werden, wie sie sich bei Verlust eines Authentisierungsmittels zu verhalten haben.

SYS.2.1.A29 Systemüberwachung und Monitoring der Clients (H)

Die Clients SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden, das den Systemzustand und die Funktionsfähigkeit der Clients laufend überwacht und Fehlerzustände sowie die Über- bzw. Unterschreitung definierter Grenzwerte an das Betriebspersonal meldet.

SYS.2.1.A30 Einrichten einer Referenzumgebung für Clients (H)

Für Clients SOLLTE eine Referenzinstallation erstellt werden, in der die Grundkonfiguration und alle Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf den Client vorab getestet werden können. Für verschie-

dene, typische und häufig wiederkehrende Testfälle SOLLTEN Checklisten erstellt werden, die beim Testlauf möglichst automatisiert abgearbeitet werden sollten. Die Testfälle SOLLTEN sowohl die Perspektive der Benutzung als auch die des Betriebs berücksichtigen. Zusätzlich SOLLTEN alle Tests so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.2.1.A31 Einrichtung lokaler Paketfilter (H)

Auf jedem Client SOLLTEN, zusätzlich zu den eingesetzten zentralen Sicherheitsgateways, lokale Paketfilter eingesetzt werden. Es SOLLTE eine Strategie zur Implementierung gewählt werden, die nur benötigte Netzkommunikation explizit erlaubt.

SYS.2.1.A32 Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits (H)

Auf den Clients SOLLTEN zusätzliche Maßnahmen zum expliziten Schutz vor Exploits (Angriffe, um Systemlücken auszunutzen) getroffen werden. Wenn notwendige Schutzmaßnahmen nicht über Funktionen des Betriebssystems umgesetzt werden können, SOLLTEN zusätzliche geeignete Sicherheitsmaßnahmen umgesetzt werden. Sollte es nicht möglich sein, nachhaltige Maßnahmen umzusetzen, SOLLTEN andere geeignete (in der Regel organisatorische) Sicherheitsmaßnahmen ergriffen werden.

SYS.2.1.A33 Einsatz von Ausführungskontrolle (H)

Es SOLLTE über eine Ausführungskontrolle sichergestellt werden, dass nur explizit erlaubte Programme und Skripte ausgeführt werden können. Die Regeln SOLLTEN so eng wie möglich gefasst werden. Falls Pfade und Hashes nicht explizit angegeben werden können, SOLLTEN alternativ auch zertifikatsbasierte oder Pfad-Regeln genutzt werden.

SYS.2.1.A35 Aktive Verwaltung der Wurzelzertifikate (H)

Im Zuge der Beschaffung und Installation des Clients SOLLTE dokumentiert werden, welche Wurzelzertifikate für den Betrieb des Clients notwendig sind. Auf dem Client SOLLTEN lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten sein. Es SOLLTE regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der Institution entsprechen. Es SOLLTEN alle auf dem IT-System vorhandenen Zertifikatsspeicher in die Prüfung einbezogen werden (z. B. UEFI-Zertifikatsspeicher, Zertifikatsspeicher von Webbrowsern etc.).

SYS.2.1.A36 Selbstverwalteter Einsatz von SecureBoot und TPM (H)

Auf UEFI-kompatiblen Systemen SOLLTEN Bootloader, Kernel sowie alle benötigten Firmware-Komponenten durch selbstkontrolliertes Schlüsselmaterial signiert werden. Nicht benötigtes Schlüsselmaterial SOLLTE entfernt werden. Sofern das Trusted Platform Module (TPM) nicht benötigt wird, SOLLTE es deaktiviert werden.

SYS.2.1.A37 Verwendung von Mehr-Faktor-Authentisierung (H)

Es SOLLTE eine sichere Mehr-Faktor-Authentisierung unter Einbeziehung unterschiedlicher Faktoren (Wissen, Besitz, Eigenschaft) für die lokale Anmeldung am Client eingerichtet werden, z. B. Passwort mit Chipkarte oder Token.

SYS.2.1.A38 Einbindung in die Notfallplanung (H)

Die Clients SOLLTEN im Notfallmanagementprozess berücksichtigt werden. Die Clients SOLLTEN hinsichtlich der Geschäftsprozesse oder Fachaufgaben, für die sie benötigt werden, für den Wiederanlauf priorisiert werden. Es SOLLTEN geeignete Notfallmaßnahmen vorgesehen werden, indem mindestens Wiederanlaufpläne erstellt, Bootmedien zur Systemwiederherstellung generiert sowie Passwörter und kryptografische Schlüssel sicher hinterlegt werden.

SYS.2.1.A39 Unterbrechungsfreie und stabile Stromversorgung (H) [Haustechnik]

Clients SOLLTEN an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV SOLLTE hinsichtlich Leistung und Stützzeit ausreichend dimensioniert sein. Clients SOLLTEN vor Überspannung geschützt werden.

SYS.2.1.A40 Betriebsdokumentation (H)

Die Durchführung betrieblicher Aufgaben an Clients bzw. Clientgruppen SOLLTE nachvollziehbar anhand der Fragen „Wer?", „Wann?" und „Was?" dokumentiert werden. Aus der Dokumentation SOLLTEN insbesondere Konfigurationsänderungen nachvollziehbar sein. Auch sicherheitsrelevante Aufgaben (z. B. wer befugt ist, neue Festplatten einzubauen) SOLLTEN dokumentiert werden. Alles, was automatisch dokumentiert werden kann, SOLLTE auch automatisch dokumentiert werden. Die Dokumentation SOLLTE vor unbefugtem Zugriff und Verlust geschützt werden. Sicherheitsrelevante Aspekte SOLLTEN nachvollziehbar erläutert und hervorgehoben werden.

SYS.2.1.A41 Verwendung von Quotas für lokale Datenträger (H)

Es SOLLTE überlegt werden, Quotas einzurichten, die den verwendeten Speicherplatz auf der lokalen Festplatte begrenzen. Alternativ SOLLTEN Mechanismen des verwendeten Datei- oder Betriebssystems genutzt werden, die Benutzende bei einem bestimmten Füllstand der Festplatte warnen oder nur noch Administrierenden Schreibrechte einräumen.

SYS.2.1.A45 Erweiterte Protokollierung (H)

Es SOLLTE auch Client-Verhalten, das nicht mit der Sicherheit direkt in Verbindung steht, protokolliert und unverzüglich (automatisiert) ausgewertet werden, um verdeckte Aktivitäten mit Bezug zu Angriffen erkennen zu können.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.2.1 *Allgemeiner Client* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.2.3 Clients unter Windows

1. Beschreibung

1.1. Einleitung

Mit Windows 10 hat Microsoft sein Client-Betriebssystem Windows an eine neue Unternehmensstrategie angepasst. Verändert hat sich insbesondere auch die grundlegende Philosophie, weg vom bisherigen Prinzip des „lokalen Betriebssystems" hin zu einer Dienstleistung („Windows as a Service"). Das bedeutet, dass das Betriebssystem neben den bisherigen Funktionen auch darüber hinausgehende, insbesondere cloudbasierte, Anwendungen enthält und deswegen auf eine enge Anbindung an die Server-Infrastruktur von Microsoft angewiesen ist. Wichtige neue Aspekte im Vergleich zu den bisherigen Windows-Versionen sind vor allem der tief verankerte und teilweise nicht beeinflussbare Datenaustausch zwischen den Clients und der Herstellerinfrastruktur sowie die zunehmende Auslagerung von sicherheitskritischen Kernbestandteilen einer Windows-Infrastruktur (z. B. Authentisierung) in die Cloud.

Mit Windows 11 wurde im Oktober 2021 eine Nachfolgeversion veröffentlicht. Diese enthält neue Funktionen, hat eine überarbeitete Bedienoberfläche und im Vergleich zu Windows 10 deutlich erhöhte Systemvoraussetzungen. Insbesondere setzt Windows 11 offiziell eine 64-Bit-fähige CPU, UEFI SecureBoot sowie ein TPM 2.0 voraus. Windows 11 ist trotz des Versionssprungs jedoch keine komplette Neuentwicklung, sondern basiert auf Windows 10. Dieser Baustein ist daher sowohl für Windows 10 als auch für Windows 11 anwendbar.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die durch und auf Windows-Clients mit Windows 10 oder 11 verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.2.3 *Clients unter Windows* ist für alle Clients anzuwenden, auf denen das Betriebssystem Microsoft Windows 10 oder 11 eingesetzt wird.

Dieser Baustein enthält spezifische Anforderungen, die zum sicheren Betrieb von Clients unter dem Betriebssystem Windows zusätzlich zu den Anforderungen aus dem Baustein SYS.2.1 *Allgemeiner Client* zu beachten und zu erfüllen sind. Für Anwendungsprogramme, die auf den Windows-Clients verwendet werden, sind die Anforderungen der entsprechenden Bausteine zu erfüllen, beispielsweise APP.1.1 *Office-Produkte* oder APP.1.2 *Webbrowser*. Beim Einsatz in einer Windows-Domäne sind die Anforderungen der entsprechenden Bausteine wie APP.2.2 *Active Directory Domain Services* zu erfüllen.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.2.2.3 *Clients unter Windows* von besonderer Bedeutung.

2.1. Schadprogramme auf Windows-Clients

Aufgrund der hohen Verbreitung von Windows-Betriebssystemen und der zwischen den Systemgenerationen oftmals vorhandenen Abwärtskompatibilität zu älteren Versionen ist die Gefährdung durch Schadprogramme und unbefugtes Eindringen in IT-Systeme für Windows vergleichsweise hoch.

2.2. Integrierte Cloud-Funktionen

Windows beinhaltet zahlreiche Funktionen, mit denen Daten unter Nutzung der Dienste von Microsoft abgelegt und synchronisiert werden („Cloud-Dienste"). Dadurch besteht die Gefahr, diese unbewusst, oder zumindest unbedacht, auch für möglicherweise institutionskritische oder personenbezogene Daten zu nutzen. Außerdem können Benutzende gegen die Datenschutzgesetze verstoßen, wenn Daten bei Dritten, in der Regel im Ausland, gespeichert werden. Meldet sich eine Person mit bereits aktiviertem Microsoft-Account an ein neues Gerät an, werden automatisch die von ihm genutzten Microsoft-Cloud-Dienste eingerichtet. So können Daten der Institution ungewollt auf die privaten Geräte der Mitarbeitenden synchronisiert werden. Als weiteres Beispiel bietet Windows als Standardeinstellung die Möglichkeit, den Bitlocker-Recovery-Schlüssel direkt über den Microsoft-Account in der Cloud zu sichern und somit schutzbedürftige kryptografische Geheimnisse in die Hände Dritter zu geben.

2.3. Beeinträchtigung von Software-Funktionen durch Kompatibilitätsprobleme

Software, die auf Vorgängerversionen eines Betriebssystems erfolgreich betrieben werden konnte, muss nicht auch grundsätzlich mit der aktuellen Version von Windows zusammenarbeiten. Mögliche Ursachen sind neue Sicherheitsmerkmale oder Betriebssystemeigenschaften sowie der Wegfall von Funktionen oder Diensten. In der Folge kann die Software nicht oder nur eingeschränkt verwendet werden. Beispiele für aktivierte Sicherheitsmerkmale, die bei neuen Windows-Versionen die Ursache für mögliche Kompatibilitätsprobleme sein können, sind die Benutzerkontensteuerung (UAC) oder, bei 64-Bit-Versionen des Betriebssystems, Kernel Patch Guard. Außerdem könnten signierte Treiber notwendig sein, die möglicherweise für ältere Geräte nicht mehr zur Verfügung stehen.

2.4. Telemetrie-Funktionen von Windows

Windows sendet standardmäßig sogenannte Diagnosedaten an den Hersteller Microsoft. Zusätzlich kann Microsoft über den in Windows integrierten Telemetrie-Dienst gezielt Informationen von einem Client abfragen. Im Telemetrie-Level „Full" bzw. „Vollständig", der in den Windows-Editionen Home und Pro der Standard-Level ist, schließt dies beispielsweise den Zugriff auf die Registry des Clients sowie die Ausführung von bestimmten Diagnosetools auf dem Client mit ein. Es besteht die Gefahr, dass die Diagnose- bzw. Telemetriedaten schützenswerte Informationen enthalten, die auf diesem Weg an Dritte gelangen können.

2.5. Eingeschränkte Forensik bei der Nutzung des Virtual Secure Mode (VSM)

Durch die Nutzung des Virtual Secure Mode (VSM) werden forensische Untersuchungen, z. B. zur Sicherheitsvorfallbehandlung, eingeschränkt bzw. erschwert. Prozesse, die durch den Secure Kernel bzw. dem Isolated User Mode (IUM) geschützt werden, sind nicht mehr zugänglich. Beispielsweise können Speicherabbilder dieser Prozesse aufgrund kryptografischer Maßnahmen nicht ausgewertet werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.2.3 *Clients unter Windows* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.2.2.3.A1 Planung des Einsatzes von Cloud-Diensten unter Windows (B)

Da Windows-basierte Geräte eng mit den Cloud-Diensten des Herstellers Microsoft verzahnt sind, MUSS vor ihrer Verwendung strategisch festgelegt werden, welche enthaltenen Cloud-Dienste in welchem Umfang genutzt werden sollen bzw. dürfen.

SYS.2.2.3.A2 Auswahl und Beschaffung einer geeigneten Windows-Version (B)

Der Funktionsumfang und die Versorgung mit funktionalen Änderungen einer Windows-Version MÜSSEN unter Berücksichtigung des ermittelten Schutzbedarfs und des Einsatzzwecks ausgewählt werden. Die Umsetzbarkeit der erforderlichen Absicherungsmaßnahmen MUSS bei der Auswahl berücksichtigt werden. Basierend auf dem Ergebnis der Überprüfung MUSS der etablierte Beschaffungsprozess um die Auswahl des entsprechenden Lizenzmodells und „Service Branches" (CB, CBB oder LTSC) erweitert werden.

SYS.2.2.3.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.2.2.3.A4 Telemetrie und Datenschutzeinstellungen unter Windows (B)

Um die Übertragung von Diagnose- und Nutzungsdaten an Microsoft stark zu reduzieren, MUSS das Telemetrie-Level 0 (Security) in der Enterprise-Edition von Windows konfiguriert werden. Wenn diese Einstellung nicht wirksam umgesetzt wird oder bei anderen Windows-Edition umgesetzt werden kann, dann MUSS durch geeignete Maßnahmen, etwa auf Netzebene, sichergestellt werden, dass die Daten nicht an den Hersteller übertragen werden.

SYS.2.2.3.A5 Schutz vor Schadsoftware unter Windows (B)

Sofern nicht gleich- oder höherwertige Maßnahmen, wie z. B. Ausführungskontrolle, zum Schutz des IT-Systems vor einer Infektion mit Schadsoftware getroffen wurden, MUSS eine spezialisierte Komponente zum Schutz vor Schadsoftware auf Windows-Clients eingesetzt werden.

SYS.2.2.3.A6 Integration von Online-Konten in das Betriebssystem (B) [Benutzende]

Die Anmeldung am System sowie an der Domäne DARF NUR mit dem Konto eines selbst betriebenen Verzeichnisdienstes möglich sein. Anmeldungen mit lokalen Konten SOLLTEN Administrierenden vorbehalten sein. Online-Konten zur Anmeldung, etwa ein Microsoft-Konto oder Konten anderer Identitätsmanagementsysteme, DÜRFEN NICHT verwendet werden, da hier personenbezogene Daten an die Systeme Dritter übertragen werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.2.3.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.2.3.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.2.3.A9 Sichere zentrale Authentisierung in Windows-Netzen (S)

Für die zentrale Authentisierung SOLLTE ausschließlich Kerberos eingesetzt werden. Eine Gruppenrichtlinie SOLLTE die Verwendung älterer Protokolle verhindern. Ist dies nicht möglich, MUSS alternativ NTLMv2 eingesetzt werden. Die Authentisierung mittels LAN-Manager und NTLMv1 DARF NICHT innerhalb der Institution und in einer produktiven Betriebsumgebung erlaubt werden. Die eingesetzten kryptografischen Mechanismen SOLLTEN entsprechend dem ermittelten Schutzbedarf und basierend auf den internen Richtlinien konfiguriert und dokumentiert werden. Abweichende Einstellungen SOLLTEN begründet und mit dem Sicherheitsmanagement abgestimmt sein.

SYS.2.2.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.2.3.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.2.3.A12 Datei- und Freigabeberechtigungen unter Windows (S)

Der Zugriff auf Dateien und Ordner auf dem lokalen System sowie auf Netzfreigaben SOLLTE gemäß einem Berechtigungs- und Zugriffskonzept konfiguriert werden. Auch die standardmäßig vorhandenen administrativen Freigaben auf dem System SOLLTEN hierbei berücksichtigt werden. Die Schreibrechte für Benutzende SOLLTEN auf einen definierten Bereich im Dateisystem beschränkt werden. Insbesondere SOLLTEN Benutzende keine Schreibrechte für Ordner des Betriebssystems oder installierter Anwendungen erhalten.

SYS.2.2.3.A13 Einsatz der SmartScreen-Funktion (S)

Die SmartScreen-Funktion, die aus dem Internet heruntergeladene Dateien und Webinhalte auf mögliche Schadsoftware untersucht und dazu unter Umständen personenbezogene Daten an Microsoft überträgt, SOLLTE deaktiviert werden.

SYS.2.2.3.A14 Einsatz des Sprachassistenten Cortana (S) [Benutzende]

Cortana SOLLTE deaktiviert werden.

SYS.2.2.3.A15 Einsatz der Synchronisationsmechanismen unter Windows (S)

Die Synchronisierung von Benutzendendaten mit Microsoft Cloud-Diensten und das Sharing von WLAN-Passwörtern SOLLTEN vollständig deaktiviert werden.

SYS.2.2.3.A16 Anbindung von Windows an den Microsoft-Store (S)

Die Verwendung des Microsoft-Stores SOLLTE auf die Verträglichkeit mit den Datenschutz- und Sicherheitsvorgaben der Institution überprüft und bewertet werden. Die generelle Installation von Apps auf Windows ist nicht von der Anbindung an den Microsoft-Store abhängig, daher SOLLTE sie, sofern sie nicht benötigt wird, deaktiviert werden.

SYS.2.2.3.A17 Keine Speicherung von Daten zur automatischen Anmeldung (S)

Die Speicherung von Kennwörtern, Zertifikaten und anderen Informationen zur automatischen Anmeldung an Webseiten und IT-Systemen SOLLTE NICHT erlaubt werden.

SYS.2.2.3.A18 Einsatz der Windows-Remoteunterstützung (S)

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTEN bei der Planung der Windows-Remoteunterstützung (hiermit ist nicht RDP gemeint) berücksichtigt werden. Eine Remoteunterstützung SOLLTE nur nach einer expliziten Einladung erfolgen. Bei der Speicherung einer Einladung in einer Datei SOLLTE diese ein Kennwort besitzen. Dem Aufbau einer Sitzung SOLLTE immer explizit zugestimmt werden. Die maximale Gültigkeit der Einladung für eine Unterstützung aus der Ferne SOLLTE in der Dauer angemessen sein. Sofern die Windows-Remoteunterstützung nicht verwendet wird, SOLLTE sie vollständig deaktiviert werden.

SYS.2.2.3.A19 Sicherheit beim Fernzugriff über RDP (S) [Benutzende]

Die Auswirkungen auf die Konfiguration der lokalen Firewall SOLLTEN bei der Planung des Fernzugriffs berücksichtigt werden. Die Gruppe der berechtigten Benutzenden für den Remote-Desktopzugriff (RDP) SOLLTE durch die Zuweisung entsprechender Berechtigungen festgelegt werden. In komplexen Infrastrukturen SOLLTE das RDP-Zielsystem nur durch ein dazwischengeschaltetes RDP-Gateway erreicht werden können. Für die Verwendung von RDP SOLLTE eine Prüfung und deren Umsetzung sicherstellen, dass die nachfolgend aufgeführten Komfortfunktionen im Einklang mit dem Schutzbedarf des Zielsystems stehen:

- die Verwendung der Zwischenablage,
- die Einbindung von Druckern,

- die Einbindung von Wechselmedien und Netzlaufwerken sowie
- die Nutzung der Dateiablagen und von Smartcard-Anschlüssen.

Sofern der Einsatz von Remote-Desktopzugriffen nicht vorgesehen ist, SOLLTEN diese vollständig deaktiviert werden. Die eingesetzten kryptografischen Protokolle und Algorithmen SOLLTEN sicher sein und den internen Vorgaben der Institution entsprechen.

SYS.2.2.3.A20 Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten (S)

Die Konfigurationsparameter der sogenannten Benutzerkontensteuerung (User Account Control, UAC) SOLLTEN für die privilegierten Konten zwischen Bedienbarkeit und Sicherheitsniveau abgewogen eingesetzt werden. Die Entscheidungen für die zu verwendenden Konfigurationsparameter SOLLTEN dokumentiert werden. Darüber hinaus SOLLTE die Dokumentation alle Konten mit Administrationsrechten enthalten sowie regelmäßig geprüft werden, ob es notwendig ist, die Rechte erweitern zu können.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.2.2.3.A21 Einsatz des Encrypting File Systems (H)

Da das Encrypting File System (EFS) die verwendeten Schlüssel mit dem Passwort des jeweiligen Kontos schützt, SOLLTE ein sicheres Passwort verwendet werden. Zusätzlich SOLLTEN restriktive Zugriffsrechte die mit EFS verschlüsselten Dateien schützen. Der Wiederherstellungsagent SOLLTE ein dediziertes Konto und kein Administrationskonto sein. In diesem Zusammenhang SOLLTE der private Schlüssel des Agenten gesichert und aus dem System entfernt werden. Es SOLLTEN von allen privaten Schlüsseln Datensicherungen erstellt werden. Beim Einsatz von EFS mit lokalen Konten SOLLTEN die lokalen Passwortspeicher mittels Syskey verschlüsselt werden. Alternativ kann der Windows Defender Credential Guard genutzt werden. Benutzende SOLLTEN im korrekten Umgang mit EFS geschult werden.

SYS.2.2.3.A22 Verwendung der Windows PowerShell (H)

Die PowerShell und die WPS-Dateien SOLLTEN nur von Administrierenden ausgeführt werden können. Die PowerShell-Ausführung selbst SOLLTE zentral protokolliert und die Protokolle überwacht werden. Die Ausführung von PowerShell-Skripten SOLLTE mit dem Befehl *Set-ExecutionPolicy AllSigned* eingeschränkt werden, um zu verhindern, dass unsignierte Skripte versehentlich ausgeführt werden.

SYS.2.2.3.A23 Erweiterter Schutz der Anmeldeinformationen unter Windows (H)

Auf UEFI-basierten Systemen SOLLTE SecureBoot verwendet und der Status des geschützten Modus für den Local Credential Store LSA beim Systemstart überwacht werden. Ist eine Fernwartung der Clients mittels RDP vorgesehen, SOLLTE beim Einsatz von Windows in einer Domäne ab dem Funktionslevel 2012 R2 von der Option „restrictedAdmin“ für RDP Gebrauch gemacht werden.

SYS.2.2.3.A24 Aktivierung des Last-Access-Zeitstempels (H)

Es SOLLTE geprüft werden, ob der Last-Access-Zeitstempel im Dateisystem aktiviert werden kann, um die Analyse eines Systemmissbrauchs zu erleichtern. Bei der Prüfung SOLLTEN mögliche Auswirkungen dieser Einstellung, wie Performance-Aspekte oder resultierende Einschränkungen bei inkrementellen Backups, berücksichtigt werden.

SYS.2.2.3.A25 Umgang mit Fernzugriffsfunktionen der „Connected User Experience and Telemetry“ (H)

Es SOLLTE berücksichtigt werden, dass die Komponente „Connected User Experience and Telemetry“ (CUET) bei Windows fester Bestandteil des Betriebssystems ist und neben der Telemetriefunktion auch eine Fernzugriffsmöglichkeit für den Hersteller Microsoft auf das lokale System erlaubt. Ein solcher Fernzugriff auf den Windows-Client SOLLTE netzseitig geloggt und falls erforderlich geblockt werden.

SYS.2.2.3.A26 Nutzung des Virtual Secure Mode (VSM) (H)

Bei der Nutzung des Virtual Secure Mode (VSM) SOLLTE berücksichtigt werden, dass forensische Untersuchungen, z. B. zur Sicherheitsvorfallbehandlung, eingeschränkt oder erschwert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI stellt im Rahmen des Projekts „SiSyPHuS Win10 (**S**tud**i**e zu **Sy**stemintegrität, **P**rotokollierung, **H**ärtung **u**nd **S**icherheitsfunktionen in Windows 10)" eine Analyse der Sicherheitsfunktionen von Windows 10 und darauf aufbauend passende Härtungsempfehlungen bereit: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/SiSyPHuS_Win10/SiSyPHuS_node.html

Der Hersteller Microsoft stellt unter anderem folgende weiterführende Informationen zu Windows bereit:

- Konfigurieren von zusätzlichem LSA-Schutz: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
- Credential Guard – Überblick: https://docs.microsoft.com/de-de/windows/access-protection/credential-guard/credential-guard-requirements
- Device Guard – Überblick: https://technet.microsoft.com/de-de/library/dn986865.aspx

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.3 Clients unter Linux und Unix

1. Beschreibung

1.1. Einleitung

Neben Windows werden auf immer mehr Clients Linux- oder seltener Unix-basierte Betriebssysteme installiert. Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Linux bezeichnet hingegen kein klassisches, sondern ein funktionelles Unix-System, da der Linux-Kernel nicht auf dem ursprünglichen Quelltext basiert, aus dem sich die verschiedenen Unix-Derivate entwickelt haben. Da sich die Konfiguration und der Betrieb von Linux- und Unix-Clients ähneln, werden in diesem Baustein Linux und Unix sprachlich als „Unix-Client" bzw. „unixartig" zusammengefasst.

Linux ist freie Software, die von der Open-Source-Gemeinschaft entwickelt wird. Das bedeutet, dass sie frei genutzt, kopiert, verteilt und verändert werden darf. Daneben gibt es Unternehmen, die den Linux-Kernel und die verschiedenen Software-Komponenten zu einer Distribution zusammenfassen und pflegen sowie weitere Dienstleistungen anbieten. Häufig werden Derivate der Distributionen Debian, Fedora / Red Hat Enterprise Linux oder openSUSE / SUSE Linux Enterprise eingesetzt. Darüber hinaus gibt es für spezielle Einsatzzwecke und Geräte zugeschnittene Linux-Distributionen. Dazu gehören z. B. Qubes OS, das versucht, ein hohes Maß an Sicherheit durch Virtualisierung zu erreichen, LibreElec für den Einsatz eines Home Theater PCs (HTPC) oder Kali Linux, eine auf Sicherheit, Computerforensik und Penetrationstests spezialisierte Distribution. Außerdem können Clients auch Live-Distributionen starten, ohne dass das auf dem Client installierte Betriebssystem verändert wird. Der Marktanteil des Betriebssystems Linux auf Clients hat in den letzten Jahren zugenommen. In speziellen Einsatzumgebungen werden weiterhin „klassische" Unix-Systeme in verschiedenen Derivaten eingesetzt. Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz betrieben.

Durch die Menge der vorausgewählten Softwarepakete einer Standardinstallation der gängigen Linux-Distributionen beziehungsweise der Unix-Derivate erhöht sich einerseits die Angriffsfläche. Gleichzeitig bieten unixartige Betriebssysteme aber auch umfangreiche Schutzmechanismen.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf Linux- und Unix-Clients erstellt, bearbeitet, gespeichert oder versendet werden. Die Anforderungen des Bausteins gelten vorrangig für Linux-Clients, können aber generell für Unix-Clients adaptiert werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.3 *Clients unter Linux und Unix* ist für alle Clients anzuwenden, auf denen Linux- oder Unix-basierte Betriebssysteme eingesetzt werden.

Dieser Baustein enthält grundsätzliche Anforderungen zum Betrieb von unixartigen Clients. Er konkretisiert und ergänzt die Aspekte, die im Baustein SYS.2.1 *Allgemeiner Client* behandelt werden, um Besonderheiten von Unix-Systemen. Dementsprechend sind die beiden Bausteine immer gemeinsam anzuwenden.

Auch wenn es sich bei macOS von Apple um ein unixartiges Betriebssystem handelt, wird dieses Betriebssystem nicht in diesem Baustein behandelt. Empfehlungen hierzu sind im Baustein SYS.2.4 *Clients unter macOS* zu finden.

Der Baustein umfasst nur das eigentliche Betriebssystem, das in der Regel bei einer Basisinstallation einer Distribution installiert wird. Darauf aufbauende Software, wie E-Mail-Clients oder Office-Software, wird in diesem Baustein nicht berücksichtigt. Anforderungen hierzu sind z. B. in den Bausteinen der Schicht APP.1 *Client-Anwendungen* des IT-Grundschutz-Kompendiums zu finden.

Dieser Client-Baustein setzt voraus, dass neben Administrierenden dauerhaft nur eine unveränderte Person mit einem interaktiven Konto aktiv ist. Clients, die von mehreren Personen nacheinander oder gleichzeitig genutzt werden, erfordern zusätzliche Maßnahmen, die im Rahmen dieses Bausteins nicht behandelt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.2.3 *Clients unter Linux und Unix* von besonderer Bedeutung.

2.1. Software aus Drittquellen

Bei unixartigen IT-Systemen kommt es vor, dass Benutzende Softwarequellcode selbst herunterladen und kompilieren, statt fertige Softwarepakete zu installieren. Wenn fertige Softwarepakete genutzt werden, werden diese außerdem in einigen Fällen aus Drittquellen ohne weitere Prüfung installiert, statt ausschließlich aus den vorhandenen Paketquellen des herstellenden Unternehmens. Jeder dieser alternativen Wege der Softwareinstallation birgt zusätzliche Risiken, da dadurch fehlerhafte oder inkompatible Software sowie Schadsoftware installiert werden kann.

2.2. Ausnutzbarkeit der Skriptumgebung

Oft werden in unixartigen Betriebssystemen Skriptsprachen genutzt. Skripte sind eine Auflistung von einzelnen Kommandos, die in einer Textdatei gespeichert und beispielsweise in der Kommandozeile aufgerufen werden. Durch den großen Funktionsumfang der Skriptumgebungen können Angreifende Skripte umfangreich für ihre Zwecke missbrauchen. Darüber hinaus können aktivierte Skriptsprachen nur sehr schwer eingedämmt werden.

2.3. Dynamisches Laden von gemeinsam genutzten Bibliotheken

Mit der Kommandozeilenoption LD_PRELOAD wird eine dynamische Bibliothek vor allen anderen Standardbibliotheken, die in einer Anwendung benötigt werden, geladen. Dadurch lassen sich gezielt einzelne Funktionen der Standardbibliotheken durch eigene überschreiben. Angreifende könnten das Betriebssystem beispielsweise so manipulieren, dass Schadfunktionen bei der Nutzung von bestimmten Anwendungen mit ausgeführt werden.

2.4. Fehlerhafte Konfiguration

Schon in einer Standardinstallation werden bei unixartigen Betriebssystemen zahlreiche Anwendungen installiert, die separat konfiguriert werden müssen. Auch nachinstallierte Anwendungen müssen separat konfiguriert werden, so dass sich schließlich unzählige Konfigurationsdateien auf dem Betriebssystem befinden.

Da viele Anwendungen unabhängig voneinander konfiguriert werden, können die Konfigurationsoptionen im Widerspruch zueinander stehen, ohne dass dies aus den einzelnen Einstellungen ersichtlich ist. Beispielsweise könnte ein Dienst für eine Fernadministration auf einem Port lauschen, der von Paketfilterregeln blockiert wird. Auf diese Weise können die Anwendungen zusätzliche Funktionen bereitstellen, die nicht gewünscht sind, oder wichtige Funktionen nicht anbieten. Das kann dazu führen, dass bestimmte Aufgaben am Client erschwert oder gar nicht erfüllt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.3 *Clients unter Linux und Unix* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.2.3.A1 Authentisierung von Administrierenden und Benutzenden (B) [Benutzende]

Personen mit Adminstrationsrechten DÜRFEN sich NICHT im Normalbetrieb als „root" anmelden. Für die Systemadministrationsaufgaben SOLLTE „sudo" oder eine geeignete Alternative mit einer geeigneten Protokollierung genutzt werden. Es SOLLTE verhindert werden, dass sich mehrere Benutzende auf einem Client gleichzeitig einloggen können.

SYS.2.3.A2 Auswahl einer geeigneten Distribution (B)

Auf Grundlage der Sicherheitsanforderungen und des Einsatzzwecks MUSS ein geeignetes Unix-Derivat bzw. eine geeignete Linux-Distribution ausgewählt werden. Es MUSS für die geplante Einsatzdauer des Betriebssystems Support verfügbar sein. Alle benötigten Anwendungsprogramme SOLLTEN als Teil der Distribution direkt verfügbar sein. Sie SOLLTEN nur in Ausnahmefällen aus Drittquellen bezogen werden. Distributionen, bei denen das Betriebssystem selbst kompiliert wird, SOLLTEN NICHT in Produktivumgebungen eingesetzt werden.

SYS.2.3.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.2.3.A4 Kernel-Aktualisierungen auf unixartigen Systemen (B)

Der Client MUSS zeitnah neu gebootet werden, nachdem der Kernel des Betriebssystems aktualisiert wurde. Ist dies nicht möglich, MUSS alternativ Live-Patching des Kernels aktiviert werden.

SYS.2.3.A5 Sichere Installation von Software-Paketen (B)

Wenn zu installierende Software aus dem Quellcode kompiliert werden soll, DARF diese NUR unter einem unprivilegierten Konto entpackt, konfiguriert und übersetzt werden. Anschließend DARF die zu installierende Software NICHT unkontrolliert in das Wurzeldateisystem des Betriebssystems installiert werden.

Wird die Software aus dem Quelltext übersetzt, dann SOLLTEN die gewählten Parameter geeignet dokumentiert werden. Anhand dieser Dokumentation SOLLTE die Software jederzeit nachvollziehbar und reproduzierbar kompiliert werden können. Alle weiteren Installationsschritte SOLLTEN dabei ebenfalls dokumentiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.3.A6 Kein automatisches Einbinden von Wechsellaufwerken (S) [Benutzende]

Wechsellaufwerke SOLLTEN NICHT automatisch eingebunden werden. Die Einbindung von Wechsellaufwerken SOLLTE so konfiguriert sein, dass alle Dateien als nicht ausführbar markiert sind (Mount-Option „noexec").

SYS.2.3.A7 Restriktive Rechtevergabe auf Dateien und Verzeichnisse (S)

Es SOLLTE sichergestellt werden, dass Dienste und Anwendungen nur die ihnen zugeordneten Dateien erstellen, verändern oder löschen dürfen. Auf Verzeichnissen, in denen alle Konten Schreibrechte haben (z. B. „/tmp"), SOLLTE das Sticky Bit gesetzt werden.

SYS.2.3.A8 Einsatz von Techniken zur Rechtebeschränkung von Anwendungen (S)

Zur Beschränkung der Zugriffsrechte von Anwendungen auf Dateien, Geräte und Netze SOLLTE App-Armor oder SELinux eingesetzt werden. Es SOLLTEN die von dem jeweiligen Unix-Derivat bzw. der Linux-Distribution am besten unterstützten Lösungen eingesetzt werden. Rechte SOLLTEN grundsätzlich entzogen sein und wo nötig über Positivlisten explizit erteilt werden.

Erweiterungen zur Rechtebeschränkung SOLLTEN im Zwangsmodus (Enforcing Mode) oder mit geeigneten Alternativen verwendet werden.

SYS.2.3.A9 Sichere Verwendung von Passwörtern auf der Kommandozeile (S) [Benutzende]

Passwörter SOLLTEN NICHT als Parameter an Programme übergeben werden.

SYS.2.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.3.A11 Verhinderung der Überlastung der lokalen Festplatte (S)

Es SOLLTEN Quotas für Konten bzw. Dienste eingerichtet werden, die ausreichend Freiraum für das Betriebssystem lassen. Generell SOLLTEN unterschiedliche Partitionen für Betriebssystem und Daten genutzt werden. Alternativ SOLLTEN auch Mechanismen des verwendeten Dateisystems genutzt werden, die ab einem geeigneten Füllstand nur noch dem Konto „root“ Schreibrechte einräumen.

SYS.2.3.A12 Sicherer Einsatz von Appliances (S)

Es SOLLTE sichergestellt werden, dass Appliances ein ähnliches Sicherheitsniveau wie Clients auf Standard-IT-Systemen erfüllen. Es SOLLTE dokumentiert werden, wie entsprechende Sicherheitsanforderungen mit einer eingesetzten Appliance erfüllt werden. Wenn die Anforderungen nicht zweifelsfrei erfüllt werden können, SOLLTE eine Konformitätserklärung von den herstellenden Unternehmen angefordert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.2.3.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.2.3.A14 Absicherung gegen Nutzung unbefugter Peripheriegeräte (H)

Peripheriegeräte SOLLTEN nur nutzbar sein, wenn sie explizit freigegeben sind. Kernelmodule für Peripheriegeräte SOLLTEN nur geladen und aktiviert werden, wenn das Gerät freigegeben ist.

SYS.2.3.A15 Zusätzlicher Schutz vor der Ausführung unerwünschter Dateien (H)

Partitionen und Verzeichnisse, in denen Benutzende Schreibrechte haben, SOLLTEN so gemountet werden, dass keine Dateien ausgeführt werden können (Mountoption „noexec“).

SYS.2.3.A16 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.2.3.A17 Zusätzliche Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (H)

Die Nutzung von Systemaufrufen SOLLTE insbesondere für exponierte Dienste und Anwendungen auf die unbedingt notwendige Anzahl beschränkt werden (z. B. durch seccomp). Die vorhandenen Standardprofile bzw. -regeln von SELinux, AppArmor sowie alternativen Erweiterungen SOLLTEN manuell überprüft und gegebenenfalls an die eigene Sicherheitsrichtlinie angepasst werden. Falls erforderlich, SOLLTEN neue Regeln bzw. Profile erstellt werden.

SYS.2.3.A18 Zusätzlicher Schutz des Kernels (H)

Es SOLLTEN mit speziell gehärteten Kernels (z. B. grsecurity, PaX) geeignete Schutzmaßnahmen wie Speicherschutz, Dateisystemabsicherung und rollenbasierte Zugriffskontrolle umgesetzt werden, die eine Ausnutzung von Schwachstellen und die Ausbreitung im Betriebssystem verhindern.

SYS.2.3.A19 Festplatten- oder Dateiverschlüsselung (H)

Festplatten oder die darauf abgespeicherten Dateien SOLLTEN verschlüsselt werden. Die dazugehörigen Schlüssel SOLLTEN NICHT auf dem IT-System gespeichert werden. Es SOLLTEN AEAD-Verfahren (Authenticated Encryption with Associated Data) bei der Festplatten- und Dateiverschlüsselung eingesetzt werden. Alternativ SOLLTE „dm-crypt" in Kombination mit „dm-verity" genutzt werden.

SYS.2.3.A20 Abschaltung kritischer SysRq-Funktionen (H)

Es SOLLTE festgelegt werden, welche SysRq-Funktionen von den Benutzenden ausgeführt werden dürfen. Generell SOLLTEN keine kritischen SysRq-Funktionen von den Benutzenden ausgelöst werden können.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.2.3 *Clients unter Linux und Unix* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.4 Clients unter macOS

1. Beschreibung

1.1. Einleitung

macOS ist ein Client-Betriebssystem der Firma Apple. macOS basiert auf Darwin, dem frei verfügbaren Unix-Betriebssystem von Apple, das wiederum auf dem Open-Source-Betriebssystem FreeBSD aufbaut. macOS setzt sich im Wesentlichen aus Darwin sowie der proprietären grafischen Bedienoberfläche „Aqua" und weiteren Anwendungen und Diensten zusammen. Gemäß den Lizenzbedingungen von Apple darf macOS nur auf IT-Systemen („Macs") von Apple installiert werden. Aus diesem Grund sind Eigenheiten dieser Systeme ebenfalls Bestandteil dieses Bausteins.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist der Schutz von Informationen, die auf IT-Systemen unter macOS verarbeitet oder mit diesen übertragen werden. Dazu müssen IT-Systeme unter macOS angemessen abgesichert werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.4 *Clients unter macOS* ist für alle Client-Systeme anzuwenden, auf denen das Betriebssystem Apple macOS eingesetzt wird.

Der Schwerpunkt liegt in diesem Baustein auf der Absicherung eines Macs mit macOS, der als Stand-alone-System oder als Client in einem Client-Server-Netz betrieben wird. Damit ergänzt der Baustein die allgemeinen Aspekte aus dem zusätzlich anzuwendenden Baustein SYS.2.1 *Allgemeiner Client*. Ein möglicher Einsatz von macOS als Server-Betriebssystem wird im Baustein nicht betrachtet. Im professionellen Einsatz besteht mit dem sogenannten Profilmanager und Mobile Device Management die Möglichkeit, die verwendeten Macs zentral zu verwalten. Diese Lösungen bieten erweiterte Konfigurations- und Verwaltungsfunktionen, werden in diesem Baustein jedoch nicht betrachtet. Entsprechende Sicherheitsaspekte werden im Baustein SYS.3.2.2 *Mobile Device Management (MDM)* behandelt. Außerdem ist zu beachten, dass die beiden Apple-Betriebssysteme macOS (für Macs) und iOS (für iPhones) bzw. iPadOS (für iPads) eng miteinander verzahnt sind. Daher sollte zusätzlich der Baustein SYS.3.2.3 *iOS (for Enterprise)* berücksichtigt werden, wenn neben macOS auch Geräte mit iOS oder iPadOS eingesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.2.4 *Clients unter macOS* von besonderer Bedeutung.

2.1. Unkontrollierbarer Zugriff auf ausgelagerte Daten

macOS bietet eine Reihe von Funktionen, die auf zentralen, von Apple betriebenen Servern ausgeführt werden. Beispielsweise kann Apples iCloud für die Speicherung und für die Synchronisierung von Daten zwischen verschiedenen macOS- und iOS-Geräten verwendet werden. Da hierbei Daten auf Servern Dritter zwischengespeichert werden und damit nicht mehr unter der eigenen Kontrolle stehen, könnten prinzipiell auch Unbefugte auf diese Server zugreifen und die dort gespeicherten oder übertragenen Daten einsehen und für ihre Zwecke missbrauchen.

2.2. Missbrauch der Apple-ID als zentrale Zugangsinformation für Apple-Dienste

Für die Nutzung einiger macOS-Funktionen wird eine eindeutige Apple-ID als Zugangsinformation benötigt. Mit der Apple-ID kann zentral auf verschiedene Apple-Dienste zugegriffen werden, wie beispielsweise auf iCloud, iMessage und den App Store. Falls Unbefugte an die Zugangsinformationen der Apple-ID gelangen, können sie diese Dienste unter Umständen unter einer falschen Identität nutzen und auf Informationen in iCloud zugreifen.

2.3. Angriffe auf Funkschnittstellen

Ein Mac verfügt in der Regel über drahtlose Schnittstellen wie WLAN oder Bluetooth, die zudem von vielen Diensten genutzt werden und entsprechend aktiviert sind. Beispielsweise können damit Dateien unmittelbar zwischen Apple-Geräten ausgetauscht werden (AirDrop). Des Weiteren kann die WLAN- und Bluetooth-Funktion genutzt werden, um macOS- und iOS-Geräte zu synchronisieren (Continuity). Mit AirPlay ist es möglich, Video- und Audiodaten an kompatible Wiedergabegeräte zu senden. Angreifende könnten versuchen, diese Funkschnittstellen für Angriffe zu missbrauchen, um vertrauliche Informationen zwischen Mac, iPhone, iPad und anderen Geräten abzufangen oder die Geräte zu kompromittieren.

2.4. Angriffe auf Anwendungen mit Vorschau-Funktion

Einige der in macOS integrierten Anwendungen unterstützen eine Vorschaufunktion für bestimmte Dateiformate (z. B. Bilddateien). Dazu gehören der Finder, der Browser „Safari" und das in macOS integrierte E-Mail-Programm. Die Vorschaufunktion stellt beispielsweise automatisch den Anhang einer E-Mail auszugsweise dar, wenn das Dateiformat bekannt ist. Angreifende könnte somit versuchen, Schadcode im Anhang einer E-Mail zu verstecken. Die Vorschaufunktion würde den E-Mail-Anhang anzeigen und möglicherweise den Schadcode ausführen, der wiederum den Mac kompromittieren könnte.

2.5. Unsichere Protokolle in macOS oder macOS-Anwendungen

macOS und seine Anwendungen unterstützen verschiedene, zum Teil Apple-eigene Protokolle (z. B. AFP) zur Kommunikation mit zentralen Servern oder anderen Endgeräten. Wenn diese Kommunikationsprotokolle keine ausreichenden Sicherheitsmechanismen aufweisen oder unsicher konfiguriert werden, könnten die darüber übertragenen Daten unerlaubt mitgelesen, verfälscht oder anderweitig missbraucht werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.4 *Clients unter macOS* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.2.4.A1 Planung des sicheren Einsatzes von macOS (B)

Die Einführung von macOS MUSS sorgfältig geplant werden. Es MUSS entschieden werden, wo und wie Daten abgelegt werden. Es MUSS geplant werden, wie die Datensicherung in das institutionsweite Datensicherungskonzept integriert werden kann. Es MUSS geplant werden, wie Sicherheits- und sonstige Aktualisierungen für macOS und Anwendungen systematisch installiert werden können. Es MUSS ermittelt werden, welche Anwendungen bei einem Plattformwechsel zu macOS benötigt werden. Wird der Mac in einem Datennetz betrieben, MUSS zusätzlich berücksichtigt werden, welche Netzprotokolle eingesetzt werden sollen.

SYS.2.4.A2 Nutzung der integrierten Sicherheitsfunktionen von macOS (B)

Die in macOS integrierten Schutzmechanismen „System Integrity Protection" (SIP), „Xprotect" und „Gatekeeper" MÜSSEN aktiviert sein. Gatekeeper DARF NUR die Ausführung signierter Programme erlauben, sofern unsignierte Programme nicht zwingend notwendig sind.

SYS.2.4.A3 Verwendung geeigneter Konten (B) [Benutzende]

Das bei der Erstkonfiguration von macOS angelegte Konto hat Administrationsrechte und DARF NUR zu administrativen Zwecken verwendet werden. Für die normale Verwendung des Macs MUSS ein Konto mit Standard-Berechtigungen angelegt werden. Sollte der Mac von mehreren Benutzenden verwendet werden, MUSS für jeden Benutzenden ein eigenes Konto angelegt werden. Das Gast-Konto MUSS deaktiviert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.4.A4 Verwendung einer Festplattenverschlüsselung (S)

Festplatten SOLLTEN, insbesondere bei mobilen Macs (z. B. MacBooks), verschlüsselt werden. Wird dazu die in macOS integrierte Funktion FileVault verwendet, DARF das Schlüsselmaterial NICHT online bei Apple gespeichert werden. Der von FileVault erzeugte Wiederherstellungsschlüssel MUSS an einem sicheren Ort aufbewahrt werden. Es SOLLTE geprüft werden, ob ein institutioneller Wiederherstellungsschlüssel für FileVault verwendet werden soll.

SYS.2.4.A5 Deaktivierung sicherheitskritischer Funktionen von macOS (S)

Die in macOS integrierten Ortungsdienste SOLLTEN deaktiviert werden. Heruntergeladene Daten SOLLTEN NICHT automatisch geöffnet werden. Inhalte von optischen und anderen Medien SOLLTEN NICHT automatisch ausgeführt werden.

SYS.2.4.A6 Verwendung aktueller Mac-Hardware (S)

Werden neue Macs beschafft, SOLLTEN aktuelle Modelle ausgewählt werden. Werden bereits vorhandene Macs eingesetzt, SOLLTE regelmäßig überprüft werden, ob diese sowie das darauf installierte Betriebssystem weiterhin von Apple mit Sicherheits-Updates versorgt werden. Werden die Macs nicht mehr durch Apple unterstützt, SOLLTEN sie nicht mehr verwendet werden.

SYS.2.4.A7 Zwei-Faktor-Authentisierung für Apple-ID (S) [Benutzende]

Die Zwei-Faktor-Authentisierung für die Verwendung des Apple-ID-Kontos SOLLTE aktiviert werden.

SYS.2.4.A8 Keine Nutzung von iCloud für schützenswerte Daten (S) [Benutzende]

Es SOLLTE verhindert werden, dass schützenswerte Daten zwischen mehreren Geräten über iCloud-Dienste synchronisiert werden. Stattdessen SOLLTEN Daten nur über selbst betriebene Dienste synchronisiert werden. Schützenswerte Daten SOLLTEN NICHT in iCloud gespeichert werden. Entwürfe, beispielsweise von E-Mails oder Dokumenten, SOLLTEN NICHT automatisch in iCloud gespeichert werden.

SYS.2.4.A9 Verwendung von zusätzlichen Schutzprogrammen unter macOS (S)

Bei Bedarf, etwa wenn Macs in einem heterogenen Netz betrieben werden, SOLLTEN neben den integrierten Schutzmechanismen von macOS zusätzlich Virenschutz-Lösungen von Drittanbietern eingesetzt werden.

SYS.2.4.A10 Aktivierung der Personal Firewall unter macOS (S)

Die in macOS integrierte Personal Firewall SOLLTE aktiviert und geeignet konfiguriert werden.

SYS.2.4.A11 Geräteaussonderung von Macs (S)

Bei einer Aussonderung des Macs SOLLTEN der nichtflüchtige Datenspeicher NVRAM (Non Volatile Random Access Memory) sowie der SMC (System Management Controller) zurückgesetzt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.2.4.A12 Firmware-Kennwort und Boot-Schutz auf Macs (H) [Benutzende]

Auf älteren Macs SOLLTE die Abfrage eines sicheren Firmware-Kennworts im sogenannten „Command-Modus“ aktiviert werden, um ein unberechtigtes Booten des Macs von einem anderen Startlaufwerk zu verhindern. Es SOLLTE geprüft werden, ob über den „Full-Modus“ ein Kennwort bei jedem Startvorgang abgefragt werden sollte.

Auf Macs mit T2-Sicherheitschip SOLLTE ein Firmware-Passwort über das Startsicherheitsdienstprogramm gesetzt werden. Die Option „Sicheres Starten: Volle Sicherheit“ SOLLTE aktiviert werden. Die Option „Starten von externen Medien nicht zulassen“ SOLLTE aktiviert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das National Institute of Standards and Technology (NIST) stellt das Dokument „SP 800-179 Rev. 1 (DRAFT): Guide to Securing Apple macOS 10.12 Systems for IT Professionals: A NIST Security Configuration Checklist“ (Oktober 2018) zur Verfügung.